REMARKS

Claims 1-41 were pending in the application. Claims 1-41 were subject to restriction. Claims 33-36 were rejected. Claims 1-32 and 37-41 are canceled. Claims 33-36 are now pending in the application. Claims 33 and 35 are the independent claims. Reconsideration of the amended application is respectfully requested.

The examiner stated that the application includes claims directed to three patentably distinct inventions. The claims, which previously had been subject to an election requirement, are now subject to a restriction requirement. In response, the applicant elects Invention III, which is recited in claims 33-36, for further examination on the merits. Claims 1-32 and 37-41 are canceled without prejudice to or disclaimer of the subject matter recited therein.

The examiner rejected claims 33 and 35 under 35 USC 112, first paragraph, as failing to comply with the enablement requirement. In particular, the examiner stated that the claim limitation "generating, by the first party, a first asymmetric key pair based on the base, prime, and sub-prime parameters, and a shared key based on the second public key" is not clearly and specifically addressed in the specification.

In the written description, public-key cryptographic schemes are described. An exemplary scheme featuring Diffie-Hellman key agreement is referenced, for example, on page 14, at lines 1-8. This scheme, which in certain embodiments makes use of base, prime, and sub-prime parameters, designated as G, P, and Q, is well-known to those of skill in the art. As noted in the written description on page 3, at lines 4-15, variations of this scheme are patented. An on-line search of the relevant literature results in numerous references. For example, the scheme is explained in terms of base, prime, and sub-prime parameters at http://www.ietf.org/rfc/rfc2631.txt. Because this scheme is well-known to those of skill in the art, numerous references are available in the prior art, and the applicant makes specific reference to the scheme in the written description, it is respectfully submitted that one of skill in the art would know how to make and use the claimed invention based on the written description provided in the specification. The rejection, therefore, should be withdrawn.

The examiner rejected claims 33 and 35 under 35 USC 112, second paragraph, as being indefinite. In particular, the examiner stated that the claim language "net label" is not specifically defined in the specification.

The written description clearly defines a "net label" as a CKM label generated at each platform involved in the secure communication of the claimed invention. For example, on page 14, at lines 7 and 8, it is stated that a pair of CKM labels can be generated by each platform. In the exemplary exchange that is described in the following passage, these labels are identified as a Net label and a Private label. CKM labels and their uses are described in the specification, for example, on page 6, line 27 through page 7, line 13. Thus, the term is specifically defined in the specification and the claim is not indefinite. The rejection, therefore, should be withdrawn.

The examiner rejected claims 33-36 under 35 USC 103 as being unpatentable over Chen et al., in view of Elgamal et al.

Independent claim 33 recites a method of establishing a secure communication channel. According to the claimed method, the following actions take place:

- A first party sends a secure call notification to a second party.

- The first and second parties access base, prime, and sub-prime parameters.

- The second party generates a second asymmetric key pair comprising a second public key and a second private key, based on the base, prime, and sub-prime parameters.

- The second party sends the second public key to the first party.

- The first party generates a net label, a private label, a random value, a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters, and a shared key based on the second public key.

- The first party encrypts the net label, the private label, and the random value, using the shared key.

- The first party sends the encrypted net label, the encrypted private label, the encrypted random value, and the first public key to the second party.

- The second party generates the shared key based on the first public key.

- The second party decrypts the encrypted net label, the encrypted private label, and the encrypted random value using the shared key.

- The first and second parties exchange respective identification numbers to establish the secure communication channel.

In contrast, Chen et al. disclose public key sterilization, by which public keys are certified. Chen et al. describe generally-known public key cryptographic concepts (column 3, line 55 through column 4, line 6), the Diffie-Hellman key exchange scheme (column 4,lines 7-63), basic encryption concepts (column 4, line 65 through column 6, line 8), and the methodology behind digital signatures (column 6, line 10 through column

7, line 3). At column 9, line 46 through column 10, line 21, Chen et al. describe a discrete logarithm public key sterilization scheme by which a user generates public and private key pairs and submits these to a certificate authority for sterilizing, that is, the certificate authority generates a second key pair based on the user's key pair, wherein the second key pair is less likely to be used in a malicious manner. Unlike the method of claim 33, a secure communication channel is not established. That is, keys are not exchanged in order to secure communication between the user and the certificate authority. Rather, the user's keys are replaced so that the user can later establish secure communication with another user.

Likewise, Chen et al. describe, at column 10, line 22 through column 11, line 25, an RSA public key sterilization scheme. Again, the user generates a public/private key pair, and transmits the key pair to the certificate authority, which generates a sterilized version of the key pair and provides this second key pair to the user. The user can then use the second key pair in place of the original key pair for secure communication with another user. Chen et al. do not disclose the formation of a secure channel between those two users, only the generation of a sterilized key for use by a user. Details of the use of the sterilized keys are limited to the Chen et al. descriptions of general encryption and digital signature processes.

As acknowledged by the examiner, Chen et al. do not disclose generating, by the first user, a net label, a private label, and a random value. Chen et al. do not disclose or suggest generating these values, because a secure channel is not being established. Elgamal et al. discloses a secure socket layer application program, that is, a channel for conducting secure transactions over a network. As noted by the examiner, Elgamal et al. disclose the transmission of challenge data from a client to a server. Elgamal states that this challenge data is a random number used to ensure channel security (column 7, lines 13-18). Thus, the challenge data does not include a net label and a private label, as asserted by the examiner. Cipher-specs are sent with the challenge data, but these are just indications of which bulk ciphers are supported by the client, and are not net labels or private labels.

Thus, Elgamal et al. fail to overcome the noted deficiencies of the Chen et al. disclosure. That is, neither reference discloses at least the use of net labels and private labels in establishing a secure communications channel. Further, even if Elgamal et al. disclosed these elements, there would be no reason for one of ordinary skill in the art to apply that teaching to the Chen et al. process, because Chen et al. do not disclose the establishment of a secure communication channel. Rather, Chen et al. disclose the generation of keys that can be used to provide reliable encryption of data and digital signatures. Chen et al. provide no motivation to one of skill in the art to secure a communications channel by creating a secure socket layer such as that disclosed by Elgamal et al. Likewise, Elgamal et al. provide no suggestion that the disclosed secure socket layer could be provided to greater advantage through the exchange of net labels and private labels.

For at least the foregoing reasons, it is submitted that no combination of the teachings of the cited references would be proper, and further that such combination still would not disclose all of the elements of claim 33, and therefore could not render obvious the invention recited by claim 33. Claims 34 depends from claim 33, and therefore also cannot be rendered obvious by the combination of the cited references. The rejections of claims 33 and 34, therefore, should be withdrawn.

Claim 35 recites a method of establishing a secure communication channel. According to the claimed method, the following actions take place:

- A communication link is established among at least three parties comprising a first party and other parties.

- The first party sends a broadcast conference call notification to the other parties.

- The first party and the other parties access base, prime, and sub-prime parameters.

- The first party generates a net label, a random value, and a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters.

- The first party sends the first public key to each of the other parties.

- Each of the other parties generates a respective private label, a respective other asymmetric key pair comprising a respective other public key and a respective other private key based on the base, prime, and sub-prime parameters, and a respective other shared key based on the first public key.

- Each of the other parties encrypts the respective private label using the respective shared key.

- Each of the other parties sends the respective encrypted private label and the respective other public key to the first party.

- The first user computes each respective shared key from each respective public key sent by the other parties.

- The first party decrypts each respective encrypted private label using the respective shared keys.

- The first user encrypts the net label and the random number, respectively, using the respective shared keys.

- The first party sends the respective encrypted net labels and the respective encrypted random values to the respective other parties.

- The other parties decrypt the respective encrypted net labels and the respective encrypted random values using the respective shared keys.

- The first user and the other users establish the secure communication channel using the net label and the random value.

In contrast, Chen et al. disclose public key sterilization, by which public keys are certified. Chen et al. describe generally-known public key cryptographic concepts (column 3, line 55 through column 4, line 6), the Diffie-Hellman key exchange scheme (column 4,lines 7-63), basic encryption concepts (column 4, line 65 through column 6, line 8), and the methodology behind digital signatures (column 6, line 10 through column 7, line 3). At column 9, line 46 through column 10, line 21, Chen et al. describe a discrete logarithm public key sterilization scheme by which a user generates public and private key pairs and submits these to a certificate authority for sterilizing, that is, the certificate authority generates a second key pair based on the user's key pair, wherein the second key pair is less likely to be used in a malicious manner. Unlike the method of claim 35, a secure communication channel is not established among three or more users. That is, keys are not exchanged in order to secure communication between the user and the certificate authority. Rather, the user's keys are replaced so that the user can later establish secure communication with another user.

Likewise, Chen et al. describe, at column 10, line 22 through column 11, line 25, an RSA public key sterilization scheme. Again, the user generates a public/private key pair, and transmits the key pair to the certificate authority, which generates a sterilized version of the key pair and provides this second key pair to the user. The user can then use the second key pair in place of the original key pair for secure communication with another user. Chen et al. do not disclose the formation of a secure channel between those two users, or among more than two users, only the generation of a sterilized key for usc by a user. Details of the use of the sterilized keys are limited to the Chen et al. descriptions of general encryption and digital signature processes.

As acknowledged by the examiner, Chen et al. do not disclose generating, by the first user, a net label, a private label, and a random value. Chen et al. do not disclose or suggest generating these values, because a secure channel is not being established. Elgamal et al. discloses a secure socket layer application program, that is, a channel for conducting secure transactions over a network. As noted by the examiner, Elgamal et al. disclose the transmission of challenge data from a client to a server. Elgamal states that this challenge data is a random number used to ensure channel security (column 7, lines 13-18). Thus, the challenge data does not include a net label and a private label, as asserted by the examiner. Cipher-specs are sent with the challenge data, but these are just indications of which bulk ciphers are supported by the client, and are not net labels or private labels.

Thus, Elgamal et al. fail to overcome the noted deficiencies of the Chen et al. disclosure. That is, neither reference discloses at least the use of net labels and private labels in establishing a secure communications channel. Further, even if Elgamal et al. disclosed these elements, there would be no reason for one of ordinary skill in the art to apply that teaching to the Chen et al. process, because Chen et al. do not disclose the establishment of a secure communication channel among three or more users. Rather, Chen et al. disclose the generation of keys that can be used to provide reliable encryption of data and digital signatures. Chen et al. provide no motivation to one of skill in the art to secure a communications channel by creating a secure socket layer such as that disclosed by Elgamal et al. Likewise, Elgamal et al. provide no suggestion that the disclosed secure socket layer could be provided to greater advantage through the exchange of net labels and private labels.

For at least the foregoing reasons, it is submitted that no combination of the teachings of the cited references would be proper, and further that such combination still would not disclose all of the elements of claim 35, and therefore could not render obvious the invention recited by claim 35. Claims 36 depends from claim 35, and therefore also cannot be rendered obvious by the combination of the cited references. The rejections of claims 35 and 36, therefore, should be withdrawn.

Based on the foregoing, it is submitted that all objections and rejections have been overcome. It is therefore requested that the Amendment be entered, the claims allowed, and the case passed to issue.

Respectfully submitted,

October 21, 2005
Date

Thomas M. Champagne
Registration No. 36,478
Customer Number 49691
(828) 253-8600

TMC:hlp